UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
09/221,869	12/29/98	LINEHAN M	SE9-98-031(1

EXAMINER	
ELISCA P	12
ART UNIT	**PAPER NUMBER**
2161	

DATE MAILED: 02/23/01

TM01/0223

STEVEN J MEYERS
IBM CORPORATION
INTELLECTUAL PROPERTY LAW BLGD 1
ROUTE 100 MP 1L1140
SOMERS NY 10589

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary	Application No. 09/221,869	Applicant(s) Linehan, Mark
	Examiner Pierre Eddy Elisca	Group Art Unit 2161

☒ Responsive to communication(s) filed on *Dec 27, 2000* .

☐ This action is **FINAL.**

☐ Since this application is in condition for allowance except for formal matters, **prosecution as to the merits is closed** in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11; 453 O.G. 213.

A shortened statutory period for response to this action is set to expire *THREE* month(s), or thirty days, whichever is longer, from the mailing date of this communication. Failure to respond within the period for response will cause the application to become abandoned. (35 U.S.C. § 133). Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

Disposition of Claims

☒ Claim(s) *1-54* is/are pending in the application.

Of the above, claim(s) _____ is/are withdrawn from consideration.

☐ Claim(s) _____ is/are allowed.

☒ Claim(s) *1-54* is/are rejected.

☐ Claim(s) _____ is/are objected to.

☐ Claims _____ are subject to restriction or election requirement.

Application Papers

☐ See the attached Notice of Draftsperson's Patent Drawing Review, PTO-948.

☐ The drawing(s) filed on _____ is/are objected to by the Examiner.

☐ The proposed drawing correction, filed on _____ is ☐approved ☐disapproved.

☐ The specification is objected to by the Examiner.

☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

☐ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

☐ All ☐ Some* ☐ None of the CERTIFIED copies of the priority documents have been

☐ received.

☐ received in Application No. (Series Code/Serial Number) _____ .

☐ received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

*Certified copies not received: _____ .

☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

☒ Notice of References Cited, PTO-892

☐ Information Disclosure Statement(s), PTO-1449, Paper No(s). _____

☐ Interview Summary, PTO-413

☐ Notice of Draftsperson's Patent Drawing Review, PTO-948

☐ Notice of Informal Patent Application, PTO-152

--- SEE OFFICE ACTION ON THE FOLLOWING PAGES ---

Examiner Pierre Eddy Elisca

United States Department of Commerce

Patent and Trademark Office

Washington, D. C. 20231

DETAILED ACTION

Response to Amendment

1. **This office action is in response to Applicant's amendment, filed on 12/27/2000.**

2. Claims 1-50 are remained and claims 51-54 are added.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. **Claims 1-14 and 16-50 are rejected under 35 U.S.C. 103 (a) as being unpatentable over Payne et al. (U.S. Pat. No. 5,715,314) in view of Elgamal (U.S. Pat. No. 5,671,279), in view of Gifford (WO 95/16971) in view of Anderson et al. (Description of Financial Agent secured**

Transactions "FAST" Authentication) in view of Financial Technology Consortion, Fourth Draft, December 2, 1998 and in view of O'Mahony et al. Electronic Payment Systems, Artech House, Inc., Norwood, MA 1997.

As per claim 1, Payne teaches an electronic network commerce system comprising the steps of:

Sending from a merchant's computer over an Internet network (col 4, lines 43-45) to a consumer's computer, a merchant message (col 5, lines 50-53). This merchant message includes a payment amount, an order description, a merchant digital signature (col 5, lines 29-46) and a timestamp (col 5, lines 39-40). **Payne** does not explicitly state that the merchant message contains a digital certificate from an acquiring bank as claimed by the Applicant. **Elgamal**, however, expressly teaches that the message from the merchant to the customer in his electronic commerce system contains a digital certificate from the acquirer (col 9, lines 55-59). It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the teachings of **Payne** by including the certificate from the acquiring bank as taught by **Elgamal** to get the invention as claimed by the Applicant. The advantage would be to provide an important form of authentication in network commerce systems (Elgamal, col 4, lines 37-42).

Payne also does not explicitly teach that the merchant message is a wallet initiation message and that this message starts a consumer's wallet program in the consumer's computer in response to the wallet initiation message. However, **O'Mahony** explicitly teaches that the merchant response from a

consumer pay message initiates a wallet program in the consumer's computer (page 79, section 4.6.3, paragraph 1, lines 1-5). It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the teachings of **Payne** with the wallet initiation message taught by **O'Mahony** for the advantage of making the purchasing steps as transparent as possible to the consumer by hiding the details of the payment steps and messages during a purchase (O'Mahony, page 78, section 4.6.1, lines 1-4).

Payne explicitly teaches sending from the consumer's computer, a message containing the consumer's identity and authentication information to a payment computer (including an issuer gateway verifies the merchant's signature to prove that the consumer is dealing with the actual merchant and validating, at the issuer gateway, the merchant's certificate and the acquirer's certificate to prove that the merchant and issuer share a common financial arrangement (col 5, lines 34-36, col 7, lines 24-27 and col 8, lines 3-5).

Payne explicitly teaches that the issuer gateway verifies the consumer's account (col 6, lines 43-56) an ensures that funds and/or credit are available to support the payment amount (col 7, lines 14-15).

Payne teaches that the payment computer (or issuer gateway) authorizes payment by sending over the Internet network an authorization token, an issuer's digital certificate, and a wallet initiation message. He also teaches that the authorization token includes the payment amount, order description, timestamp, a merchant identifier and a reference to the consumer's credit or debit card number (col 7, lines 14-30).

Payne, however, does not explicitly state that the payment authorization massage (or token) contains a random nonce, but **Gifford** explicitly teaches issuing a payment order that includes a random nonce as claimed by the Applicant (page 4, lines 21-28). It would have been to a person of ordinary skill in the art at the time of the invention to modify the teachings of **Payne** including a nonce in the payment authorization as taught by **Gifford** for the advantage of preventing a replay attack on the payment system (see., page 48, section 3.11 of O'Mahony).

Payne explicitly teaches that nonce the merchant's computer receives the authorization token, the order description is fulfilled (col 7, line 49).

Based on the amendment filed 08/09/2000, Applicant added the limitation of forming a four party payment protocol for electronic sales. The four party payment protocol includes a consumer computer connected to a merchant and an issuing gateway. The four party payment protocol also includes a merchant computer connected to an acquirer bank and the consumer computer via the Internet. According to **O'Mahony**, an issuer bank is a bank licensed by one of the major credit card companies (i.e., Visa or Master card) that issues credit cards to customers. **O'Mahony** also states that merchants that wish to accept credit card payments must register with bank which is called the acquiring bank or simply the acquirer (section 2.3, pages 12 and 13). Fig 2.3 on page 13 of **O'Mahony** shows the connection of the consumer to the issuer and the connection between the merchant and the acquiring bank as claimed by the Applicant. Applicant also states that the connection is accomplished via a gateway connection. According to the Computer Dictionary Third Edition, Microsoft Press, 1997, page 215) a gateway is a device that connects network using different

communications protocols so that information can be passed from one to the other. Accordingly, Applicant's addition of forming a four party payment protocol for electronic sales, the four party payment protocol including a consumer's computer coupled to a merchant's computer and it an issuing bank computer via an issuer gateway, the merchant computer being further coupled to an acquirer bank computer is just a description of connection topology used fro credit card payments and is a well known and was commonly used at the time of the invention. Adding the description of a well known payment topology to the claim limitations already covered in the previous Office Action does not overcome the rejection of claim 1.

Based on the amendment filed 12/27/2000, Applicant added the limitation the issuer bank creating a reference number or value representing the consumer's credit or debit card number by preparing a table of credit card or debit card numbers and a corresponding table of reference numbers, the issuing bank pairing the consumer's card number with a selected reference number and outputting the reference number to the issuer gateway. However, this limitation has been taught by Payne in col 6, lines 31-42, wherein said the buyer computer sends payment URL B to the payment computer (step 62).....).

As per claim 2, Payne expressly states that a start message is sent from consumer's computer over the internet network to the merchant's computer, to initiate the merchant's message (fig 2A, number 32).

As per claim 3, Payne teaches that the message received from the merchant in response to a buy message contains digital signature from the merchant (col 5, lines 42 and 43). **Payne** does not explicitly teach that the digital signature contains a nonce as claimed by the Applicant. **Elgamal**, however, explicitly teaches that the message sent from the merchant to the consumer is also signed by the merchant (col 9, lines 56-60) and the signature contains a nonce (col 8, line 16). It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the teachings of **Payne** with the inclusion of the nonce in the message sent from the merchant to the consumer as taught by **Elgamal** for the advantage of preventing a replay attack. The limitation that this message is a wallet initiation message was already covered in he rejection of claim 1 above.

As per claim 4, Payne explicitly teaches that the merchant's computer further performs the steps of receiving the authorization token (fig 2H, number 92); verifying the issuer's signature, digital certificate, the payment amount and merchant identity in the authorization token (fig 2H, number 94); verifying the freshness of the authorization token via the timestamp in the token (fig 2H, number 98); and fulfilling the order description (fig 2I, number 102). **Payne** does not explicitly state that a nonce in the authorization token is used to recognize duplicate tokens as claimed by the Applicant. O'Mahony teaches that a nonce is used to recognize duplicate tokens (page 48, section 3.11 of **O'Mahony)**. Therefore, it would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the teachings of **Payne** by using a nonce as taught by **O'mahony** for the advantage of preventing a replay attack on the payment system.

As per claim 5, Payne explicitly teaches the use of a userid and a password to identify the consumer (col 6, lines 43 and 44).

As per claim 6, Payne teaches that the consumer interacts with a payment computer in his network sales system, but does not explicitly state that the payment computer is an ATM or a bank. Anderson teaches that FAST establishes a connection between the customer and the customer's bank by using a login and password (page 3, section 4.2). It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the teachings of Payne with the payment computer being the customer's bank as taught by Anderson for the advantage of using an existing financial institution that is familiar to the customer. Official Notice is also taken that both the concept and advantages of a bank using an ATM account debit card and password are well known and expected in the banking arts. It would have been obvious to use an ATM debit card number and PIN to identify a consumer because ATM accounts and PIN are a very common way for bank customers to interact with their bank and would avoid the confusion of creating multiple access accounts for the bank and the bank's customers.

As per claim 7-13 describe a plurality of cryptography ways to authenticate the consumer's identity in the claimed payment protocol. Official Notice is taken that both the concept and advantages of the various ways to authenticate customers in a payment system as itemized in claims 7-13 are well known and expected in the payment and cryptography arts. It would have been obvious to have

provided these authentication methods because establishing the identity of a party in a payment system is an essential element in any payment system (see., O'mahony, pages 19 and 31).

As per claim 14, Payne explicitly teaches that the issuer gateway sends the authorization token to the consumer and the consumer forwards the authorization token to the merchant (col 7, lines 31-33).

As per claim 16, Payne explicitly teaches the use of an alias card number that is mapped at the issuing bank to a real card number thereby preventing use of the consumer's credit card number without the authorization token (fig 7, col 6, lines 15-29).

As per claim 17, Payne not expressly state the use of an authorization number in the message sent back to the merchant. Gifford teaches the use of an authorization number allocated uniquely by the issuer gateway for each authorization (page 6, lines 20-23). Gifford also teaches that the issuing bank maintains a database mapping of authorization numbers to card numbers, so that when the issuing bank receives the capture message, it uses the database mapping to determine the consumer's card number (page 15, lines 16-27, fig 13). It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the teachings of Payne with the authorization number system taught by Gifford for the ad vantage of providing added security for users who are reluctant to use their actual credit card numbers over the payment network.

As per claim 18, Payne does not expressly state the use of an authorization token containing a dummy number for use in routing payment to an appropriate one of a plurality of issuing banks, such that the dummy card number is shared among all card holders of a particular issuing bank. Official Notice is taken that both the concept and advantages of using a dummy number are well known and expected in the credit card and banking arts. It would have been obvious to use such a number because it would increase the efficiency of transmitting the electronic payment instructions through existing clearing house systems.

As per claims 19-23, Official Notice is taken that both the concept and advantages of using various authorization certificate hierarchies are well known and expected in the electronic commerce arts. It would have been obvious to include the various certificate arrangements cited in claims 19-23 in order to make sure that all parties in the payment protocol are trusted and are who the claim to be in any transaction

As per claim 24, Payne not explicitly teach the payment protocol for the case of a split shipment as claimed by the Applicant. Elgamal specifically covers the payment protocol for split shipments as claimed by the Applicant (col 13, line 64 through col 14, line 7). It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the teachings of Payne with the split shipment payment protocol taught by Elgamal for the advantage of handling partial shipments.

As per claim 25, Payne teaches that his sales system can buy a plurality of products and add these products to a shopping cart (col 7, line 55 through col 8, line 2), but he does not explicitly disclose "Japanese Payment Options" (installment Payments) as claimed by the Applicant. Elgamal explicit teaches that his payment protocol covers periodic payment (col 13, lines 53-63). It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the teachings of **Payne** with the periodic payment capability taught by **Elgamal** for the advantage of making car payment or other periodic payments.

Claims 26-28 are apparatus and program code claims that contain the same limitations already covered in the rejection of claim 1, so the same rejection apply to these claims. **Payne also discloses the new added limitation merchant sending a capture request message including the reference number representing the consumer's card number over the internet to an acquirer gateway operating on behalf of an acquirer bank to capture the transaction and disburse payment to the merchant (see., col 6, lines 16-59). And Elgamal discloses the step of settling the account with issuing bank (see., 11, lines 43 through col 12, line 63.**

Claims 29-31 contain the same limitations already covered in the rejections of claim 2, 3 and 4 respectively, so the same rejections apply to the rejections of claims 29-31.

As per claim 32, Payne teaches an account number associated with the payment computer, but does not explicitly teach using the consumer's credit or debit card number as claimed by the Applicant. **Elgamal**, however, explicitly teaches including the consumer's credit or debit card account number in the payment instruction message (col 10, lines 1-33). It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the teachings of **Payne** by referring to the actual consumer's credit or debit account number as taught by **Elgamal** for the advantage of being able to directly access the consumer's account without having to go through an intermediary account translation file.

Claim 33 contains the same method steps already covered in the rejection of claim 1, so the same rejections apply to the rejection of his claim. The Applicant, however, includes one additional limitation concerning the use of a URL to identify the network location of the acquiring bank contacted via an Internet network as part of the payment protocol. Official Notice is taken that both the concept and advantages of using a URL to locate a particular location on the Internet are well known and expected in the Internet and network communication arts, because the URL address structure has been used on the Internet since its inception.

Claim 34 contains the same limitations already covered in the rejections of claims 1, 7-10, 18 and 23-26, so the same rejections apply to the rejection of this claim.

Claim 35 contains the same limitations already covered in the rejections of claims 1 and 19, so the same rejections apply to the rejection of this claim.

Claim 36 contains the same limitations already covered in the rejections of claims 1 and 19-23, so the same rejections apply to the rejection of this claim.

Claims 37-39 contains the same limitations already covered in the rejections of claims 3, 4, and 32, so the same rejections apply to the rejection of this claim.

As per claim 40-42, Payne teaches the sales process but does not cover the steps necessary for a capture process in a payment protocol. Elgamal, however, covers the capture process steps as claimed by the Applicant in claim 40-42 (col 11, line 43 through col 12, line 63). It would have been obvious to a person of ordinary skill in the art at the time the invention to modify the teachings of Payne with the capture process taught by Elgamal for the advantage of actually settling the account between buyers and merchants as is common practice in almost any payment protocol.

As per claim 43, Payne explicitly teaches hashing the order information before it is sent to the merchant and also teaches that the hashing function is known by the payment computer and the merchant (col 7, line 65 through col 8, line 2). Official Notice is taken that both the concept and advantages of the merchant validating that the authorization tokens to the same order description by

comparing the hash of the order description in the authorization token against a locally-computed hash of the same order description are well known and expected in the cryptography arts. The very nature of hashing is to assure that the hashed data has not been altered by comparing the sent hash value to the hash value obtained by the recipient of the data.

Claim 44 contains the same limitations already covered in the rejections of claim 32, so the same rejections apply to the rejection of this claim.

As per claim 45, Official Notice is taken that both the concept and advantages of using higher-level security protocols such as SSL are well known and expected in the encryption arts. It would have been obvious to use higher-level security protocols such as SSL because it would allow the payment protocols to be used open public networks such as the internet. In fact SSL was developed for secure communication on the Internet (see., O'Mahony, page 72, second paragraph).

As per claims 46-50, these claims contain the same limitations already covered in the rejection of claim 1, so the same rejection applies to claim 46-50.

5. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Payne, Elgamal, Gifford, Anderson and O'Mahony, as applied to claim 1 above, and further in view of Ogram (U.S. Pat. No. 5,822,737).

As per claim 15, Payne teaches that the payment computer sends a redirect message to the buyer computer and his message is forwarded to the merchant computer (col 7, lines 31-33). **Payne** goes on to teach that a portion of the information contained in the message forwared to the merchant is encrypted so the only the payment computer and the merchant can view the contents of the message (col 7, lines 24-30). Since the encrypted portion of the message is only viewable by the payment computer and the merchant, this portion of the message would inherently be sent directly to the merchant as claimed by the Applicant. Payne, however, does not explicitly show a direct connection from the payment computer to the merchant as claimed by the Applicant. **Ogram** explicitly shows the direct connection between the payment computer and the merchant (fig 2D). It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the teachings of Payne with the direct connection taught by Ogram for the advantage of making sure the message went through when the customer's computer was disconnected and the payment computer was ready to send information intended specifically for the merchant.

6. Claims 51-54 are rejected under 35 U.S.C. 103 (a) as being unpatentable over Payne et al. (U.S. Pat. No. 5,715,314) in view of Elgamal (U.S. Pat. No. 5,671,279), in view of Gifford (WO 95/16971) in view of Anderson et al. (Description of Financial Agent secured Transactions "FAST" Authentication) in view of Financial Technology Consortion, Fourth Draft, December 2, 1998 and in view of O'Mahony et al. Electronic Payment Systems, Artech House, Inc., Norwood, MA 1997.

Claim 51 is a method's claim that contains the same limitations already covered in the rejection of claim 1, so the same rejection applies to claim 51

As per claim 52-54 Payne teaches the claimed limitations as stated in claim 1 above. Payne fails to teach the step of settling accounts with the issuing bank by the acquiring bank. Elgamal, however, covers the settling process (col 11, line 43 through col 12, line 63). It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the teach of Payne with the capture process taught by Elgamal for the advantage of actually settling the account between buyers and merchants as is common practice in almost any payment protocol.

Conclusion

7. The prior art made of record and relied upon is considered to applicant's disclosure.

Any inquiry concerning this communication from the examiner should be directed to Pierre Eddy Elisca at (703) 305-3987. The examiner can normally be reached on Monday, Tuesday, and Wednesday from 5:30AM. to 6:00PM.

If any attempt to reach the examiner by telephone is unsuccessful, the examiner's supervisor, James Trammell can be reached on (703) 305-9769.

Any response to this action should be mailed to:

Commissioner of patents and Trademarks

Washington, D.C. 20231

or faxed to:

(703) 308-9051, (for formal communications intended for entry)

OR:

(703) 305-3718 (for informal or draft communications, pleased label

"PROPOSED" or" DRAFT")

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington. VA., Sixth floor (receptionist).

JAMES P. TRAMMELL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Pierre Eddy Elisca

Patent Examiner

February 16, 2001